FortiOS - Release Notes

Version 6.4.3

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

October 22, 2020
FortiOS 6.4.3 Release Notes
01-643-655918-20201022

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-10-22	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 6.4.3 build 1778.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.4.3 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-5001D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F
FortiGate Rugged	FGR-60F
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special notices

CAPWAP traffic offloading

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip. The following models are affected:

- FG-900D
- FG-1000D
- FG-2000E
- FG-2500E

FortiClient (Mac OS X) SSL VPN requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

Tags option removed from GUI

The Tags option is removed from the GUI. This includes the following:

- The *System* > *Tags* page is removed.
- The *Tags* section is removed from all pages that had a *Tags* section.
- The *Tags* column is removed from all column selections.

System Advanced menu removal (combined with System Settings)

Bug ID	Description
584254	• Removed *System* > *Advanced* menu (moved most features to *System* > *Settings* page). • Moved configuration script upload feature to top menu > *Configuration* > *Scripts* page. • Removed GUI support for auto-script configuration (the feature is still supported in the CLI). • Converted all compliance tests to security rating tests.

PCI passthrough ports

Bug ID	Description
605103	PCI passthrough ports order might be changed after upgrading. This does not affect VMXNET3 and SR-IOV ports because SR-IOV ports are in MAC order by default.

FG-80E-POE and FG-81E-POE PoE controller firmware update

FortiOS 6.4.0 has resolved bug 570575 to fix a FortiGate failing to provide power to ports. The PoE hardware controller, however, may require an update that must be performed using the CLI. Upon successful execution of this command, the PoE hardware controller firmware is updated to the latest version 2.18:

```
diagnose poe upgrade-firmware
```

AWS-On-Demand image

Bug ID	Description
589605	Starting from FortiOS 6.4.0, the FGT-VM64-AWSONDEMAND image is no longer provided. Both AWS PAYG and AWS BYOL models will share the same FGT-VM64-AWS image for upgrading and new deployments. Remember to back up your configuration before upgrading.

Azure-On-Demand image

Bug ID	Description
657690	Starting from FortiOS 6.4.3, the FGT-VM64-AZUREONDEMAND image is no longer provided. Both Azure PAYG and Azure BYOL models will share the same FGT-VM64-AZURE image for upgrading and new deployments. Remember to back up your configuration before upgrading.

Changes in CLI

Bug ID	Description
640620	In the `wireless-controller arrp-profile` configuration, the `include-weather-channel` and `include-dfs-channel` options have changed from `yes`/`no` to `enable`/`disable`.
657726	Remove option to rate images by URL for web filter profile in the GUI and CLI.

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description
477886	PRP support for SoC4: • Configure ingress port to allow the PRP trailer to not be stripped off when the PRP packets come in. • Configure egress port to allow the PRP trailer to not be stripped off when the PRP packets go out. `config system npu` `set prp-port-in "port1"` `set prp-port-out "port2"` `end`
611992	Add a specific `auth-timeout` field in the SSL VPN monitor.
621725	Add settings to enable flow control and pause metering. Pause metering allows the FortiSwitch to apply flow control to ingress traffic when the queue is congested and to resume once it is cleared.
628963	When 802.1x authentication requests to a RADIUS server time out, the `authserver-timeout` settings within the `switch-controller security-policy 802.1x` will assign the port to a timeout VLAN.
634357	Add NPU support for GTP-U encapsulated in IPv6.
641077	After authorizing a FortiAP, administrators can also register the FortiAP to FortiCloud directly from the FortiGate GUI.
647800	AWS and Azure now support FIPS ciphers mode.
649075	FortiGate-VMs on AWS now use Amazon EC2 instance metadata service version 2 (IMDSv2) to query and retrieve metadata from the AWS cloud.
651866	FortiSwitch logs now appear as its own subtype, `switch-controller`, in event logs.
652003	In a tenant VDOM, allow `lldp-profile` and `lldp-status` to be configurable on a leased switch port.
652225	Configuring the DiffServ code in phase 2 of an IPsec tunnel allows the tag to be applied to the ESP packet. NPU offloading must be disabled for this tunnel.
652503	By configuring the service chain and service index, NSX-T east-west traffic can be redirected to a designated FortiGate VDOM. `config nsxt setting` `set liveness {enable | disable}` `set service <service name>` `end` `config nsxt service-chain`

Bug ID	Description
	`` edit <ID> set name <chain name> config service-index edit <forward index> set reverse-index <value> set name <index name> set vd <VDOM> next end next end ``` The default value for `reverse-index` is 1. The `vd` setting is required.
655920	Support 802.11v load balancing and optimized roaming.
655931	Adaptive radio architecture (ARA) allows FortiAPs to calculate the network coverage factor (NCF) based on interference on the 2.4 GHz radio. When dynamic radio mode assignment (DRMA) is enabled, if interference crosses a threshold, the radio becomes redundant by moving from AP mode to monitor mode. ``` config wireless-controller wtp-profile edit <profile> config radio-1 set band 802.11n/g-only set drma {enable | disable} set drma-sensitivity {high | medium | low} end next end ```
656039	Allow SD-WAN duplication rules to specify SD-WAN service rules to trigger packet duplication. This allows SD-WAN duplication to occur based on an SD-WAN rule instead of the source, destination, or service parameters in the duplication rule.
657598	In an application control list, the `exclusion` option allows users to specify a list of applications they wish to exclude from an entry filtered by category, technology, or others. ``` config application list edit <list> config entries edit 1 set category <ID> set exclusion <signature ID> ... <signature ID> next end next end ```
658525	The limit of BGP paths that can be selected and advertised has increased to 255 (originally 8).

Bug ID	Description
659127	Add support to deploy FortiGate-VMs that are paravirtualized with SR-IOV and DPDK/vNP on OCI shapes that use Mellanox network cards.
659346	Add additional information such as DHCP server MAC, gateway, subnet, and DNS to wireless DHCP logs.
660273	By default, the FortiGate uses the outbound interface's IP to communicate with a FortiSwitch managed over layer 3. The `switch-controller-source-ip` option allows the switch controller to use the FortiLink fixed address instead.
661131	Enabling IGMP snooping on an SSID allows the wireless controller to detect which FortiAPs have IGMP clients. The wireless controller will only forward a multicast stream to the FortiAP where there is a listener for the multicast group.
663530	IoT background scanning is disabled by default. Users can enable this option on the *FortiLink Interface* page in the GUI or with the `switch-controller-iot-scanning` in the CLI.
665735	The user device store allows user and device data collected from different daemons to be centralized for quicker access and performance: `diagnose user-device-store device memory list` `diagnose user-device-store device memory query mac <value>` `diagnose user-device-store device memory query ip <value>` `diagnose user-device-store device disk list` `diagnose user-device-store device disk query <SQL WHERE clause>`
668362	Support multiple LDAP server configurations for Kerberos keytab and agentless NTLM domain controller in multiple forest deployments.
668991	In multi-VDOM mode, security rating reports can be generated under the global scope against all VDOMs on the device.

Upgrade Information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

Device detection changes

In FortiOS 6.0.x, the device detection feature contains multiple sub-components, which are independent:

- Visibility – Detected information is available for topology visibility and logging.
- FortiClient endpoint compliance – Information learned from FortiClient can be used to enforce compliance of those endpoints.
- Mac-address-based device policies – Detected devices can be defined as custom devices, and then used in device-based policies.

In 6.2, these functionalities have changed:

- Visibility – Configuration of the feature remains the same as FortiOS 6.0, including FortiClient information.
- FortiClient endpoint compliance – A new fabric connector replaces this, and aligns it with all other endpoint connectors for dynamic policies. For more information, see Dynamic Policy - FortiClient EMS (Connector) in the *FortiOS 6.2.0 New Features Guide*.
- MAC-address-based policies – A new address type is introduced (MAC address range), which can be used in regular policies. The previous device policy feature can be achieved by manually defining MAC addresses, and then adding them to regular policy table in 6.2. For more information, see MAC Addressed-Based Policies in the *FortiOS 6.2.0 New Features Guide*.

If you were using device policies in 6.0.x, you will need to migrate these policies to the regular policy table manually after upgrade. After upgrading to 6.2.0:

1. Create MAC-based firewall addresses for each device.
2. Apply the addresses to regular IPv4 policy table.

In 6.4.0, device detection related GUI functionality has been relocated:

1. The device section has moved from *User & Authentication* (formerly *User & Device*) to a widget in *Dashboard*.
2. The email collection monitor page has moved from *Monitor* to a widget in *Dashboard*.

FortiClient Endpoint Telemetry license

Starting with FortiOS 6.2.0, the FortiClient Endpoint Telemetry license is deprecated. The FortiClient Compliance profile under the Security Profiles menu has been removed as has the Enforce FortiClient Compliance Check option under each interface configuration page. Endpoints running FortiClient 6.2.0 now register only with FortiClient EMS 6.2.0 and compliance is accomplished through the use of Compliance Verification Rules configured on FortiClient EMS 6.2.0 and enforced through the use of firewall policies. As a result, there are two upgrade scenarios:

- Customers using only a FortiGate device in FortiOS 6.0 to enforce compliance must install FortiClient EMS 6.2.0 and purchase a FortiClient Security Fabric Agent License for their FortiClient EMS installation.
- Customers using both a FortiGate device in FortiOS 6.0 and FortiClient EMS running 6.0 for compliance enforcement, must upgrade the FortiGate device to FortiOS 6.2.0, FortiClient to 6.2.0, and FortiClient EMS to 6.2.0.

The FortiClient 6.2.0 for MS Windows standard installer and zip package containing FortiClient.msi and language transforms and the FortiClient 6.2.0 for macOS standard installer are included with FortiClient EMS 6.2.0.

Fortinet Security Fabric upgrade

FortiOS 6.4.3 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 6.4.3
- FortiManager 6.4.3
- FortiClient EMS 6.4.1 build 1498 or later
- FortiClient 6.4.1 build 1519 or later
- FortiAP 6.0.6 build 0075 or later
- FortiSwitch 6.0.6 build 0076 or later

When upgrading your Security Fabric, devices that manage other devices should be upgraded first. Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. FortiGate devices
4. Managed FortiSwitch devices
5. Managed FortiAP devices
6. FortiClient EMS
7. FortiClient
8. FortiSandbox
9. FortiMail
10. FortiWeb
11. FortiADC
12. FortiDDOS
13. FortiWLC

14. FortiNAC
15. FortiVoice

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.4.3. When Security Fabric is enabled in FortiOS 6.4.3, all FortiGate devices must be running FortiOS 6.4.3.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.4.3 uses the `ssl-min-proto-version` option (under `config system global`) to control the minimum SSL protocol version used in communication between FortiGate and third-party SSL and TLS services.

When you upgrade to FortiOS 6.4.3 and later, the default `ssl-min-proto-version` option is TLS v1.2. The following SSL and TLS services inherit global settings to use TLS v1.2 as the default. You can override these settings.

- Email server (`config system email-server`)
- Certificate (`config vpn certificate setting`)
- FortiSandbox (`config system fortisandbox`)
- FortiGuard (`config log fortiguard setting`)
- FortiAnalyzer (`config log fortianalyzer setting`)
- LDAP server (`config user ldap`)
- POP3 server (`config user pop3`)

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Amazon AWS enhanced networking compatibility issue

With this enhancement, there is a compatibility issue with 5.6.2 and older AWS VM versions. After downgrading a 6.4.3 image to a 5.6.2 or older version, network connectivity is lost. Since AWS does not provide console access, you cannot

recover the downgraded image.

When downgrading from 6.4.3 to 5.6.2 or older versions, running the enhanced NIC driver is not allowed. The following AWS instances are affected:

C5	Inf1	P3	T3a
C5d	m4.16xlarge	R4	u-6tb1.metal
C5n	M5	R5	u-9tb1.metal
F1	M5a	R5a	u-12tb1.metal
G3	M5ad	R5ad	u-18tb1.metal
G4	M5d	R5d	u-24tb1.metal
H1	M5dn	R5dn	X1
I3	M5n	R5n	X1e
I3en	P2	T3	z1d

A workaround is to stop the instance, change the type to a non-ENA driver NIC type, and continue with downgrading.

FortiLink access-profile setting

The new FortiLink `local-access` profile controls access to the physical interface of a FortiSwitch that is managed by FortiGate.

After upgrading FortiGate to 6.4.3, the interface `allowaccess` configuration on all managed FortiSwitches are overwritten by the default FortiGate `local-access` profile. You must manually add your protocols to the `local-access` profile after upgrading to 6.4.3.

To configure `local-access` profile:

```
config switch-controller security-policy local-access
    edit [Policy Name]
        set mgmt-allowaccess https ping ssh
        set internal-allowaccess https ping ssh
    next
end
```

To apply `local-access` profile to managed FortiSwitch:

```
config switch-controller managed-switch
    edit [FortiSwitch Serial Number]
        set switch-profile [Policy Name]
        set access-profile [Policy Name]
    next
end
```

FortiGate VM with V-license

This version allows FortiGate VM with V-License to enable `split-vdom`.

To enable `split-vdom`:

```
config system global
   set vdom-mode [no-vdom | split vdom]
end
```

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix Hypervisor 8.1 Express Edition

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V Server 2019 and Windows Server 2012R2 with Hyper-V role

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiGuard update-server-location setting

The FortiGuard `update-server-location` default setting is different between hardware platforms and VMs. On hardware platforms, the default is `any`. On VMs, the default is `usa`.

On VMs, after upgrading from 5.6.3 or earlier to 5.6.4 or later (including 6.0.0 or later), `update-server-location` is set to `usa`.

If necessary, set `update-server-location` to use the nearest or low-latency FDS servers.

To set FortiGuard `update-server-location`:

```
config system fortiguard
   set update-server-location [usa|any]
end
```

FortiView widgets

Monitor widgets can be saved as standalone dashboards.

There are two types of default dashboard settings:

- Optimal: Default dashboard settings in 6.4.1
- Comprehensive: Default Monitor and FortiView settings before 6.4.1

Filtering facets are available for FortiView widgets in full screen and standalone mode.

WanOpt configuration changes in 6.4.0

Port configuration is now done in the profile protocol options. HTTPS configurations need to have certificate inspection configured in the firewall policy.

In FortiOS 6.4.0, `set ssl-ssh-profile certificate-inspection` must be added in the firewall policy:

```
config firewall policy
    edit 1
        select srcintf FGT_A:NET_CLIENT
        select dstintf FGT_A:WAN
        select srcaddr all
        select dstaddr all
        set action accept
        set schedule always
        select service ALL
        set inspection-mode proxy
        set ssl-ssh-profile certificate-inspection
        set wanopt enable
        set wanopt-detection off
        set wanopt-profile "http"
        set wanopt-peer FGT_D:HOSTID
```

```
    next
end
```

IPsec interface MTU value

IPsec interfaces may calculate a different MTU value after upgrading from 6.2.

This change might cause an OSPF neighbor to not be established after upgrading. The workaround is to set `mtu-ignore` to `enable` on the OSPF interface's configuration:

```
config router ospf
    config ospf-interface
        edit "ipsce-vpnx"
            set mtu-ignore enable
        next
    end
end
```

HA role wording changes

The term master has changed to primary, and slave has changed to secondary. This change applies to all HA-related CLI commands and output. The one exception is any output related to VRRP, which remains unchanged.

Product integration and support

The following table lists FortiOS 6.4.3 product integration and support information:

Web Browsers	• Microsoft Edge 83 • Mozilla Firefox version 82 • Google Chrome version 86 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 44 • Mozilla Firefox version 74 • Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Fortinet Security Fabric upgrade on page 15. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. FortiOS 6.4.3 must work with FortiManager 6.4.1 or later. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Fortinet Security Fabric upgrade on page 15. For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient: • **Microsoft Windows** • **Mac OS X** • **Linux**	• 6.2.0 See important compatibility information in FortiClient Endpoint Telemetry license on page 15 and Fortinet Security Fabric upgrade on page 15. FortiClient for Linux is supported on Ubuntu 16.04 and later, Red Hat 7.4 and later, and CentOS 7.4 and later. If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 5.6.0 and later are supported.
FortiClient iOS	• 6.2.0 and later
FortiClient Android and FortiClient VPN Android	• 6.2.0 and later
FortiClient EMS	• 6.4.0
FortiAP	• 5.4.2 and later • 5.6.0 and later
FortiAP-S	• 5.4.3 and later • 5.6.0 and later
FortiAP-U	• 5.4.5 and later
FortiAP-W2	• 5.6.0 and later

FortiSwitch OS (FortiLink support)	• 3.6.9 and later
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
FortiSandbox	• 2.3.3 and later
Fortinet Single Sign-On (FSSO)	• 5.0 build 0294 and later (needed for FSSO agent support OU in group filters) • Windows Server 2019 Standard • Windows Server 2019 Datacenter • Windows Server 2019 Core • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core • Windows Server 2008 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 Core (requires Microsoft SHA2 support package) • Novell eDirectory 8.8
FortiExtender	• 3.2.1
AV Engine	• 6.00154
IPS Engine	• 6.00058
Virtualization Environments	
Citrix	• Hypervisor 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS, 4.15.0-72-generic, QEMU emulator version 2.11.1 (Debian 1:2.11+dfsg-1ubuntu7.21)
Microsoft	• Windows Server 2012R2 with Hyper-V role • Windows Hyper-V Server 2019
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, and 6.7
VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel 82599 • Intel X540 • Intel X710/XL710

Language support

The following table lists language support information.

Language support

Language	GUI
English	✔
Chinese (Simplified)	✔
Chinese (Traditional)	✔
French	✔
Japanese	✔
Korean	✔
Portuguese (Brazil)	✔
Spanish	✔

SSL VPN support

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 82 Google Chrome version 86
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 82 Google Chrome version 86
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54
macOS Catalina 10.15	Apple Safari version 13 Mozilla Firefox version 82 Google Chrome version 86
iOS	Apple Safari Mozilla Firefox

Operating System	Web Browser
	Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

Resolved issues

The following issues have been fixed in version 6.4.3. For inquires about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
560044	Secondary device blades occasionally report critical log event `Scanunit initiated a virus engine/definitions update`. Affected models: FG-5K, 6K, and 7K series.
635365	FortiGate enters conserve mode.

Data Leak Prevention

Bug ID	Description
616918	DLP cannot detect attached ZIP and PDF files when receiving emails via MAPI over HTTPS.

DNS Filter

Bug ID	Description
649985	FortiGuard SDNS server rating timeout.

Explicit Proxy

Bug ID	Description
644121	Explicit proxy error 504, DNS fails for a specific domain.
650540	FortiGate sends traffic to an incorrect port using a wrong source NAT IP address.

Bug ID	Description
654211	When the category proxy address is applied in a proxy policy, if SOCKS traffic passes through the web proxy, when matching the SOCKS traffic with the proxy address, the WAD will crash with signal 11 at wad_url_choose_cate. Browsers may send SOCKS traffic in the background from time to time.
660703	Using the HTTP explicit proxy denies access to non-HTTP traffic and displays a policy violation.

Firewall

Bug ID	Description
586764	Abnormal prolonged CPU spike with cmdbsvr and WAD processes when making change to large policy list (10 000+ policies).
586995	Cluster VDOM policy statistics data is not correct when VFID is different for same VDOM on primary/secondary.
609027	SCTP secondary path not working in ECMP context; incorrect expectation session created from auxiliary session.
616220	ICMP reply packets dropped by the FortiGate.
635074	Firewall policy `dstaddr` does not show virtual server available based on virtual WAN link member.
643446	Fragmented UDP traffic is silently dropped when fragments have different ECN values.
644225	Challenge ACK is being dropped.
647410	`append` command allows mixing VIP and firewall address as destination objects in a firewall policy.
648951	External threat feed entry `0.0.0.0/0` shows as invalid but it blocks traffic.
650700	There should be an event log when there are internet service remove/merge entries.
650867	Firewall does not track UDP sessions on the same port.
656678	Different ciphers for SSL/HTTPS virtual servers.
659142	TNS connection request limited to 500 per second when client is trying to reach database server through the firewall.
660461	Configuration changes take a long time, and ipsmonitor and cmdbsrv processes go up to 100% of CPU.

FortiView

Bug ID	Description
643198	*Threats* drilldown for *Sources*, *Destinations*, and *Country/Region* (1 hour, 24 hours, 7 days) gives *Failed to retrieve FortiView data* error.

GUI

Bug ID	Description
446427	Failed to update VDOM license in GUI if the new license has lower VDOM count than the current license.
543192	Source IP is not used if using the GUI to query FortiGuard filtering service.
547123	The help message of `gui-dynamic-profile-display` is not correct.
561889	Firewall address object in GUI is not displaying *Invalid Subnet Mask* error when it should.
588159	When disabling *Allow Endpoint Registration*, creating a FortiClient dialup VPN with the wizard gives *Unable to setup VPN* error after completing the wizard.
606814	Security profile group does not switch from *certificate-inspection* to *no-inspection* in the GUI.
612066	*Entry not found* error shown when adding SSL VPN tunnel interface to *Multicast*.
634550	GARP is not sent when moving a virtual cluster in the GUI.
638752	All httpsd stuck in zombie state and unable to access web GUI management.
645606	`virtual-wan-link` can be set as `dstinf` in an SSL VPN policy via CLI, but it is invisible in the GUI.
646327	GUI does not show URL filter when there is a large number of URL filters.
649027	CPU usage in FortiSwitch pane is shown as 90% but checking it in the CLI shows 25%.
650307	When an external FortiGuard category is set to SSL-exempt, after clicking *Apply*, the configuration is saved in the CLI and not in the GUI.
650800	Error when deleting multiple phase 2 selectors for VPN from the GUI.
651412	Print option on *Guest Management* page does not work; send options for SMS and email are OK.
651711	Unable to select address group under SSL VPN *Source IP Pools*.
652394	Unable to change web-based email category action in DNS filter.
652975	Cannot access FortiGate by IPv6 GUI after configuring IPv6 for the first time.
653240	*Web Filtering* and *Anti-Spam* status is down on *FortiGuard* page after refreshing the page.

Bug ID	Description
653422	Unable to edit a remote user group for *Administrators* user management in global VDOM, and get *Invalid LDAP server* error.
654018	Quarantine monitor not showing quarantined IPs.
654186	In *Device Inventory Monitor* dashboard, no device information shown in inventory chart when visualization set to table.
654250	Firewall HTTPS/HTTP RADIUS authentication with password renewal does not work.
654256	*Interfaces* speed test fails and get *Failed Dependency* error when it has multiple VDOMs.
654339	Interface page keeps loading when doing a search.
654626	It is impossible to change the Action setting using the *FortiGuard Category Based Filter* on a *DNS Filter Profile* page.
655255	GUI IPv4 policy and other menus slow to load due to FortiGuard product API timing out.
655568	GUI does not allow users to deselect *Administrative Access* options for VLAN interfaces.
655891	Web CLI console does not work if port 8080 is being used.
656139	Table column is blank after changing an interface to *any* for multicast, NAT64, and NAT46 policies.
656429	FortiLink flapping and causing csfd and httpsd to crash while using high CPU.
656974	`ip6-mode` was changed from `delegated` to `static` after a parameter was changed from the GUI.
657322	`outbreak-prevention` setting is not automatically configured when enabling *Use External Malware Block List* in the GUI.
657545	Static route *Dynamic Gateway* toggle does not enable the dynamic gateway in the configuration.
661582	FortiGate Cloud logging *Date/Time* filter does not work.
663737	Add filtering facets back to FortiView widgets when using full screen or standalone mode.
663956	Unable to load web CLI console for LDAP admin with space in name.

HA

Bug ID	Description
421335	Get one-time hasync crash when running HA scripts for FIPS-CC.
637711	CSR on cluster primary is generating out-of-sync alerts on secondary and tertiary units.
640327	Duplicate logs are created by both primary and secondary devices for IPsec VPN.
643958	Inconsistent data from FFDB caused several confsyncd crashes.
647679	Inconsistent values for HA cluster inside the SNMP.

Bug ID	Description
651674	Long sessions lost on new primary after HA failover.
654341	The new join-in secondary chassis failed to sync, while primary chassis has 6K policies in one VDOM.
656099	The mgmt interfaces are excluded for heartbeat interfaces (even if `dedicate-mgmt` is not enabled).
657376	VLAN interfaces are created on a different virtual cluster primary instead of the root primary do not sync.
662893	HA cluster goes out of sync if SAML SSO admin logs in to the device.

Intrusion Prevention

Bug ID	Description
655371	Logging is intermittent for FortiGate IDS passive in one-armed sniffer mode.
660111	SSL VPN web mode IPS detection with HTTP does not work, even though it works with HTTPS.

IPsec VPN

Bug ID	Description
592361	Cannot pass traffic over ADVPN if: `tunnel-search` is set to `nexthop`, `net-device disable`, `mode-cfg enable`, and `add-route disable`.
614483	Add IKEv2 phase 2 initiator traffic selector narrowing for Cisco compatibility.
638352	In extreme situations when thousands of tunnels are negotiating simultaneously (IKEv2), iked process gets exhausted and stuck.
638573	FortiGate is not deleting the shortcut tunnel for ISPA (primary ISP) when ISPA is down.
639806	User name log empty when IPsec dialup IKEv2 has client RSA certificate with empty subject.
646012	IPsec over DHCP randomly does not work (`net-device disable`).
647285	After HA failover, not all tunnels come up; unknown SPI.
650599	IKE HA sync truncates phase 2 option flags after the first eight bits.
655739	`local-gw` is replaced with primary IP on a secondary device when the secondary IP is used as a `local-gw`.
659535	IPsec in SD-WAN and zone causes IKE crash.

Bug ID	Description
660472	Could not locate phase 1 configuration for IPv6 dialup IPsec VPN.
666693	If NAT-T IP changes, the dynamic IPsec spoke add route entry is stuck on hub.

Log & Report

Bug ID	Description
642941	For URLs over 66 characters, the FortiGate replaces remaining characters with dots (.) in `dstname` field when forwarded to syslog/FortiAnalyzer.
643840	`vwlservice` should log the SD-WAN rule and not an internet service; impacts FortiAnalyzer SD-WAN monitor widgets and reports.
645914	Move `eventtime` field to the beginning of the log to save performance on Splunk or other logging systems.
647741	On FG-60F, logging and FortiCloud reporting incorrect IPv6 bandwidth usage for sessions with NPU offload.
650325	miglogd crashes with signal 11 (segmentation fault).
651581	FortiGate tried to connect to FortiGate Cloud with the primary IP after reboot, although the secondary IP is the source in the FortiGuard log.
654363	Traffic log shows *Policy violation* for traffic hitting the allow policy in NGFW policy mode.
658665	Cannot retrieve logs from FortiAnalyzer on non-root VDOM.

Proxy

Bug ID	Description
550350	Should not be able to set `inspection-mode proxy` with IPS-enabled only policy.
579902	SSL handshake not successful with 0xc02b cipher.
619707	WAD memory leak with explicit proxy and more than 30 users.
633108	Specific WAD crashes.
638039	Delete validation is not working for *Protecting SSL Server* profile.
648831	WAD memory leak on FortiOS 6.2.4.
653099	URL filter wildcard in proxy mode.
655356	Unable to access a published website when the firewall policy is in proxy mode.

Bug ID	Description
656830	FortiGate should be in SSL bypass mode for TLS 1.2 certificate inspection with client certificate request.
658654	Cannot access specific website using proxy-based UTM with certification inspection.
660857	Unable to access some websites when proxy inspection is used in the policy.
663088	Application control in Azure fails to detect and block SSH traffic with proxy inspection.
666522	Proxy mode is blocking web browsing for some websites.
666686	Websites loading slowly with web filter applied in proxy mode.

Routing

Bug ID	Description
585816	SD-WAN route selection does not use the most specific route in the routing table when selecting the egress path.
613716	SSL VPN sends packet using wrong interface that causes disconnections.
639884	`diagnose ip proute match` gives wrong result when VRF is configured.
641050	Need support for SSL VPN web mode traffic to follow SD-WAN rules/policy route.
644461	Unable to redistribute BGP into OSPF based on community (in VRF 0).
649558	ISDB policy routes are not removed when the SD-WAN member is down.
654482	SD-WAN route tag is removed with multiple BGP paths in place.
655447	BGP prefix lifetime resets every 60 seconds when scanning BGP RIB.
655480	Upgrading to FortiOS 6.4.2 breaks all SD-WAN performance SLAs that use HTTP.
660285	Editing an existing route map rule to add `set-weight 0` results in `unset set-weight` behavior.
660300	Application vwl signal 11 (segmentation fault) received.
660311	Application vwl signal 6 (aborted) received.
661769	SD-WAN rule disappears when an SD-WAN member experiences a problem.
662655	The OSPF neighborship cannot be established; get MD5 authentication error.
662845	HA secondary also sends SD-WAN `sla-fail-log-period` to FortiAnalyzer.
663057	IPv6 routing does not work properly to be a dual stack.
666829	The bfdd process crashes.

Security Fabric

Bug ID	Description
649344	When viewing CSF child *Dashboard > WiFi* from parent FortiGate, GUI reports, *Cannot read property 'spectrum_analysis' of undefined*.
652737	FortiGate does not send interface configuration to FortiIPAM.
653368	Root FortiGate fails to load Fabric topology if HA downstream device has a trusted device in both primary and secondary FortiGates.
660250	The ipamd process is causing high memory usage.

SSL VPN

Bug ID	Description
548599	SSL VPN crash on some special URLs.
613733	Access problem for website.
615453	WebSocket using Socket.IO could not be established through SSL VPN web mode.
620793	A page inside a bookmark not opening in SSL VPN web mode.
630771	SSL VPN rewrites the URL inside the emails sent in Outlook (webmail).
637217	Internal webpage, di***, is not loading in web mode.
641379	Internal SharePoint 2019 website cannot be accessed in SSL VPN web portal.
642838	Redirected URLs do not work in web mode.
645973	Content from internal Microsoft Dynamics CRM cr***.local portal is not loading properly in SSL VPN web mode.
646295	When DNS domain is configured, requests with NTLM of host name-only bookmark could not get response from server.
647202	fas crashes when using FortiToken Cloud to access SSL VPN tunnel.
648433	Internal website loading issue in SSL VPN web portal.
649130	SSL VPN log entries display users from other VDOMs.
649193	Apache Guacamole is vulnerable to CVE-2020-9497 and CVE-2020-9498.
652060	BMC Remedy Mid Tier 9.1 web app is not displayed properly in SSL VPN web mode.
652070	BMC Remedy Mid Tier 8.1 web application elements are not displayed properly in SSL VPN web mode.
652762	SSL VPN web mode HTTPS bookmark fails to load (times out).

Bug ID	Description
652880	SSL VPN crashes around the same time that LDAP connection errors are logged.
653349	SSL VPN web mode not working for internal website.
654534	SAML authentications occurring through SSL VPN web mode are not completing.
655374	SSL VPN web portal bookmark not loading internal web page after login credentials are entered.
657689	The system allows enabling split tunnel when the SSL VPN policy is configured with destination `all`. It is not consistent with 5.6.x and 6.0.x.
657890	Internal website, https://*.da***.cz, is not working correctly in SSL VPN web mode due to source link error.
658036	When adding an FTP link to download FortiClient and accessing it through the portal, the colon is dropped from the string.
659234	FortiGate keeps replying to an ARP request for an IP address that was once assigned to an SSL VPN user, who has already disconnected and been deleted.
659312	Unable to load HTTPS bookmark in Safari (`TypeError: 'text/html'`).
659481	Internal websites not displayed successfully in SSL VPN web portal.
661372	SSL VPN incorrectly rewrites the script URL.
661835	ASUS ASMB9-iKVM application shows blank page in SSL VPN web mode.
662042	The https://outlook.office365.com and https://login.microsoft.com websites cannot be accessed in the SSL VPN web portal.
663298	The internal website is not working properly using SSL VPN.
663433	SSL VPN web mode cannot open DFS shared subdirectories, get *Invalid HTTP request* error as sslvpnd adds `NT`.
664804	User cannot use column header for data sorting (bookmark issue).
665879	When sslvpn processes the HTTP/HTTPS response with content disposition, it will change the response body since the content type is HTML.
666194	WALLIX Manager GUI interface is not loading through SSL VPN web mode.

Switch Controller

Bug ID	Description
649913	HA cluster not synchronizing when configuring an active LACP with MCLAG via FortiManager.
652745	Compatibility issues with FortiGate in 6.0 branch and FortiSwitch 424E-Fiber.

System

Bug ID	Description
581496	FG-201E stops sending out packets and NP6lite is stuck.
582536	Link monitor behavior is different between FGCP and SLBC clusters.
585882	Error in log, `msg="Interface 12345678001-ext:64 not found in the list!"`, while creating a long name VDOM in FG-SVM.
594577	Out-of-order packets for an offloaded multicast stream.
598464	Rebooting FG-1500D in 5.6.x during upgrade causes an L2 loop on the heartbeat interface and VLAN is disabled on the switch side.
603194	NP multicast session remains after the kernel session is deleted.
609660	NPU offloading enabled dropping traffic from IPsec VPN tunnel remote gateway.
627236	TCP traffic disruption when traffic shaper takes effect with NP offloading enabled.
627269	Wildcard FQDN not resolved on the secondary unit.
630146	FG-100F memory configuration check.
631132	Symantec connector does not work if management VDOM is not root vdom and root VDOM has no network connection.
631296	Forward or local bi-directional traffic from NPU inter-VDOM links through separate VDOMs is subject to high latency.
631689	FG-100F cannot forward fragmented packets between hardware switch ports.
633827	Errors during fuzzy tests on FG-1500D.
636999	LTE does not connect after upgrading from 6.2.3.
637014	Uncertified status of firmware after GUI upgrade, checksums are null.
637983	FG-100F memory configuration check fails because of wrong threshold.
642005	FortiGate does not send `service-account-id` to FortiManager via fgfm tunnel when FortiCloud is activated directly on the FortiGate.
642327	FortiGate unable to boot with kernel panic by cmdbsvr when VLAN is configured on redundant interface with non-NPU port.
642958	FG-80E terminates the firewall session abruptly when the end-users download large files.
644380	FG-40F/60F kernel panic: `failure at mm/vmalloc.c:1341/__get_vm_area_node()!`.
645723	Cannot set overlap IP on global level if `allow-subnet-overlap` on management VDOM is disabled.
648014	FortiGate DDNS failure every two months.

Bug ID	Description
648083	cmdbsvr crashed with signal 11 (segmentation fault) received.
650878	DHCP relay will honor the broadcast flag set to 0 (unicast) in only one VDOM at a time in a multi-VDOM environment.
653289	FortiExtender virtual interface cannot get IP after rebooting the system.
654159	NP6Xlite traffic not sent over the tunnel when NPU is enabled.
654624	Error message shown (`get_ha_sync_obj_sig_4dir delete broken symbolic link /etc/cert/ca/5c44d531.0`) when upgrading from 6.4.1.
657632	IPv6 passes though the DNS filter with application control enabled.
659539	FortiGate running 6.4.2 GA cannot validate license via FortiManager due to FortiManager hardware missing Fortinet_CA2 and Fortinet_SUBCA2001.
661784	FortiGuard DDNS is unable to update the renewed public IP address to the FortiGuard server.
662208	Configuration changes take a long time and cmdbsrv processes use up to 100% CPU.
662239	FGR-60F-3G4G hardware switch span does not work.
665000	HA LED off issue on FG-1100E/1101E models in 6.0.x.
668218	SD-WAN HTTP health check does not work for URLs longer than 35 characters.

Upgrade

Bug ID	Description
646877	FortiOS allows the elimination of interfaces, although it still has a VIP reference used in firewall policies.
656869	FG-100F/101F may continuously boot upon upgrading from FortiOS 6.4.0. **Workaround**: back up the 6.4.0 configuration, perform a clean install via TFTP of FortiOS 6.4.2, and restore the 6.4.0 configuration.

User & Authentication

Bug ID	Description
643191	FSSO TS-Agent is not working properly when FortiGates use NGFW policy-based mode.
655422	A space after a comma within `CN` is incorrectly removed during the bind request causing authentication failure (LDAP).

Bug ID	Description
656118	Password displayed as clear text in FortiManager installation log when resetting the system admin user password via FortiManager.
658794	FortiGate sent CSR certificate instead of signed certificate to FortiManager when retrieve is performed.
659456	REST API authentication fails for API user with PKI group enabled due to fnbamd crash.
662391	Persistent sessions for de-authenticated FSSO users.
663399	`interface-select-method` not working for RADIUS configuration.

VM

Bug ID	Description
640532	ESXi 6.0 gets `Kernel panic - not syncing: Attempted to kill init!` message.
645798	In FG-VM64-HV, `portX: can not set mac address(16).` error displayed in console after HA is enabled and all interfaces lose connections.
647800	Merge FIPS ciphers to 6.4.3 and 6.6 trunk (visible to AWS and Azure only).
652416	AWS Fabric connector always uses root VDOM even though it is not a management VDOM.
657785	On FG-AWS, changing health check protocol to `tcp-connect` causes kernel panic and reboot.
662969	Azure SDN connector filter count is not showing a stable value.
663276	After cloning the OCI instance, the OCID does not refresh to the new OCID.
663487	Should add router policy in `vdom-exception` list.
668131	EIP is not updating properly on FG-VM Azure.
670166	FG-VM64-KVM configuration revisions lost after upgrading from 6.2.5 to 6.4.2.

Web Filter

Bug ID	Description
587018	Add URL flow filter counters to SNMP.
610553	User browser gets URL block page instead of warning page when using HTTPS IP URL.
650916	Loopback interface as source IP is not getting applied to FortiGuard web filter rating.
654160	Web filter profile count decreased after upgrading to 6.4.0 on FG-100F.

Bug ID	Description
654675	Unable to get complete output of `diagnose test application ipsufd 1`.
655972	Custom category action set to allow in web filter profile causes the URL to use the FortiGuard category rather than the custom category.
661713	Global web filter profile is not applied after changes to allowed/blocked categories.

WiFi Controller

Bug ID	Description
647703	HTTPS server certificate is not presented when WiFi controller feature is disabled in *Feature Visibility*.
655689	Wireless hostapd daemon crashes upon WPA3-SAE connection.
656804	Spectrum analysis disable/enable command removed in CLI from `wtp-profile` and causing a bottleneck for APs, such as FAP-222C/223C at 100% CPU.
657391	FG-600E has cw_acd crash with `*** signal 8 (Floating point exception) received ***` in 6.2.4.
660991	FAP-U431F cannot view what channel is operating, and the override channel setting must be unset to change to a different channel.
665766	Client failed to connect SSID with WPA2-Enterprise and user group authentication.

Known issues

The following issues have been identified in version 6.4.3. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Endpoint Control

Bug ID	Description
664654	EMS host tags are not synced with the FortiGate when the user connects to a tunnel mode SSID.

Firewall

Bug ID	Description
653897	VIPs are removed from policy destination address after upgrading to 6.4.1.
666612	Get internet service name configuration error on version 7.01011 when FortiGate reboots or upgrades.

FortiView

Bug ID	Description
660753	Incorrect drilldown details shown when filtering by subnet on realtime FortiView.

GUI

Bug ID	Description
567996	GUI issues with physical topology on *Managed FortiSwitch* and *FortiSwitch Ports* pages.
650708	*Guest Management* user expiry date and time in the GUI does not match the entries in the CLI.
662873	Editing the LDAP server in the GUI alters the configuration, and `set server-identity-check disable` is removed from the LDAP configuration.
663351	RADIUS CHAP test in GUI starts failing after upgrading to 6.4.2.

HA

Bug ID	Description
615001	LAG does not come up after link failed signal is triggered.
653642	FortiGate HA failover from FortiManager is not successful.

Intrusion Prevention

Bug ID	Description
654307	Wrong direction and banned location by quarantine action for `ICMP.Oversized.Packet` in NGFW policy mode.

IPsec VPN

Bug ID	Description
644780	Rectify the consequences if password renewal on FortiClient is canceled.
652774	OCVPN spoke-to-spoke communication intermittently fails with mixed topology where some spokes have two ISPs and some have one, but the hubs have two.
655895	Unable to route traffic to a spoke VPN site from the hub FortiGate when the dialup IPsec VPN interface is dual stacked (IPv4/IPv6).

Log & Report

Bug ID	Description
661040	Cyrillic characters not displayed properly in local reports.

Routing

Bug ID	Description
654032	SD-WAN IPv6 route tag command is not available in the SD-WAN services.

SSL VPN

Bug ID	Description
550819	guacd is consuming too much memory and CPU resources during operation.

Switch Controller

Bug ID	Description
607753	CAPWAP is not updated to be a Fabric connection after upgrading from 6.4.0 Beta1 build 1519 to build 1538.

System

Bug ID	Description
464340	EHP drops for units with no NP service module.
555616	TCP packets sent out wrong interface and have high CPU usage.
587824	Member of virtual WAN link lost after upgrade if management interface is `set dedicated-to management` before.
607565	Interface `emac-vlan` feature does not work on SoC4 platform.
630861	Support FortiManager when `private-data-encryption` is enabled in FortiOS.
644782	A large number of detected devices causes httpsd to consume resources, and causes low-end devices to enter conserve mode.
647309	Kernel crash at `filter4` module and subsequent loop of `failure at mm/vmalloc.c:1341/__get_vm_area_node()!`.
651103	FG-101F crashed and rebooted when adding `vlan-protocol 8021ad` VLAN.
657629	FG-101F cannot retrieve power fan status and BGP status via SNMP.
662681	Policy package push from FortiManager fails the first time, and succeeds the second time if it is blank or has no changes.
663083	Offloaded traffic from IPsec crossing the NPU VDOM link is dropped.
666030	Empty firewall objects after pushing several policy deletes.

Upgrade

Bug ID	Description
618809	Boot up may fail when downgrading from FOS 6.4.0 to 6.2.3.

User & Authentication

Bug ID	Description
580391	Unable to create MAC address-based policies in NGFW.

VM

Bug ID	Description
596742	Azure SDN connector replicates configuration from primary device to secondary device during configuration restore.
617046	FG-VMX manager not showing all the nodes deployed.
639258	Autoscale GCP health check is not successful (port 8443 HTTPS).
646161	FG-VM with 8 CPU does not recognize all memory allocated in Hyper-V.
669822	Hot adding multiple CPUs at once to Xen-flavored VMs can result in a kernel panic crash. **Workaround**: add one CPU at a time. Alternatively, shut down the VM, add the CPUs, and restart the VM.

WiFi Controller

Bug ID	Description
643854	Client traffic was dropped by CAPWAP offloading when it connected from a mesh leaf Forti-AP managed by a FWF-61F local radio.
672136	Log severity for wireless events in Forti-WiFi and Forti-AP should be reconsidered for CAPWAP teardown.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.